2016

TERMINAL AGENCY COORDINATOR MANUAL

KANSAS HIGHWAY PATROL

KANSAS CRIMINAL JUSTICE INFORMATION SYSTEM

TABLE OF CONTENTS

TERMINAL AGENCY COORDINATOR (TAC) DUTIES & RESPONSIBILITIES 3

TRAINING 4

PERSONNEL SCREENING 7

STANDARD OPERATING PROCEDURES 9

DISSEMINATION 15

AUTHORIZED ACCESS BY A COURT 18

ENTERING NEW USERS IN KACIS 19

ASSIGNING AND ACTIVATING TOKENS 20

SELECTING A PIN 21

NAME CHANGES AND RE-HIRED EMPLOYEES 21

ASSIGN SECURITY ROLES IN OPENFOX CONFIGURATOR 22

REMOVING A USER 23

ORDERING TOKENS 23

KACIS AGENCY ADMINISTRATION 24

OPENFOX ARCHIVE AND RETRIEVAL CLIENT 25

CJIS LAUNCH PAD 25

NCIC VALIDATION PROCEDURES 31

TERMINAL USERS AGREEMENTS 32

KCJIS AGENCY CONTACT CHANGE FORM (KCJIS188) 33

PUBLIC SAFETY INFORMATION SHARING NETWORK (Nlets) 33

Terminal Agency Coordinator (TAC) Duties & Responsibilities

Each agency with KCJIS terminal access is required to have a person assigned as a TAC.
Each agency may also assign a maximum of two alternate TAC's.

TAC duties include:

- Overseeing the usage and administration of the Kansas Criminal Justice Information System (KCJIS) for your agency, to ensure all KCJIS policies are strictly adhered to.

- Serve as the agency point of contact for matters concerning KCJIS and the National Crime Information Center (NCIC), if applicable, as well as being your agency's point of contact for personnel issues.

- Monitor the KCJIS website for current KCJIS and NCIC publications and distribute the information to users of the system at your agency, and any served agency.

- The monthly validation of agency records entered into NCIC and/or the Kansas Warrant File.

- TAC & alternate TAC(s) must attend formal TAC training classes. Refresher training must be attended on a biennial basis.

- For agencies having access to NCIC, oversees NCIC certifications and re-certifications for your agency.

- Coordinate agency's KCJIS terminal requests and manage the terminal users for the agency. Enter new users into KACIS, OpenFox Configurator and the nexTEST application for your agency, as well as notify the regional KHP Trainer/Auditor.

- Inform the KHP of changes in your agency head within five (5) working days and within three (3) days of an agency TAC, alternate TAC or LASO change by means of the *KCJIS188* form which must be completed and faxed to KHP GHQ CJIS Unit.

- Assign and administer your agency's SecurID tokens used for KCJIS access. Monitor the use of the tokens. Assist the KHP and/or KBI with any inquiry involving the misuse of tokens.

- Assist the KHP Training and Audit Unit with your agency's triennial, special or random audits.

- Assuring agency personnel have access to, have read and understand the on line NCIC Operating and Code Manuals.

TRAINING

Criminal Justice Training

Criminal justice agencies shall adopt CHRI training programs. According to *Title 28*, "Each employee working with or having access to Criminal History Record Information (CHRI) shall be made familiar with the substance and intent of these regulations." Inadequate training in privacy, security, completeness and accuracy of criminal history record information by an administrator of those who must access the information may result in the finding by a court that breach of a specific duty has occurred, and the persons involved are liable for damages under the general principles of tort law. The S.O.P. shall contain an organized training program that will include relevant federal, state and agency rules and regulations regarding physical security and the collection and dissemination of criminal history records. All employees with access to CHRI records and equipment shall be required to read all relevant security rules and instructions and sign or initial the material indicating that they have read and understood them.

In order to verify that an employee has been trained in specific areas, it is required that documentation of the training shall be incorporated into the agency training and personnel records.

Your agency training program shall include physical security of the KCJIS system and the information obtained from it. Having KCJIS workstations in an unsecured environment may result in the integrity of your agency's information coming into question, possible unauthorized queries to the information and/or possible inappropriate dissemination of the information.

As appropriate, the training program shall include the agency's requirements and procedures for entry and removal of file records, as well as general access of NCIC. Agency entry worksheets are an audit requirement to be kept in the supporting case files and they shall be incorporated into the agency policy and procedures. Compliance with NCIC requirements of complete and accurate entries implies that an agency's emphasis on the required documentation, proofing of entries and validation procedures shall be addressed in the S.O.P. Reliance on NCIC manuals may be included on a secondary basis.

Agency standards and procedures relating to personnel security shall be in written form and made available to all employees. Employees and other individuals who are allowed to perform duties on behalf of a criminal justice agency in such a manner that may expose them to Criminal Justice Information (CJI) in the course of their duties, to include reserves, interns, volunteers, consultants, vendors and contractors, are required to read the standards and certify in writing that they are aware and understand them. The standards shall be included in a formal *Security Awareness Statement* in which employees and these other individuals certify in writing that they understand security violations may result in disciplinary action or, depending on the type of information, may be subject to civil and criminal penalties including a fine not to exceed $11,000 and may be considered grounds for immediate dismissal. The presentation of the *Security Awareness Statement* will be incorporated as part of the initial hiring process and may be accomplished by either the LASO or the TAC biennially. However, per CJIS Policy, it is ultimately the responsibility of the Local Agency Security Officer (LASO) rather than the TAC to ensure security awareness training has occurred and is documented.

Terminal Agency Coordinator Training

Terminal Agency Coordinator training is conducted several times each year at various locations across the state by KHP CJIS Unit personnel. Every new TAC and alternate TAC must attend this training at the next reasonably available class. Biennial refresher training for the TAC and alternate TAC(s) is also required. All KCJIS related training can be found on the CJIS Launch Pad: https://cjisaudit.khp.ks.gov/launchpad/.

Training Goal

To provide training and materials for the TAC which will convey a complete understanding of requirements set forth by CJIS, KCJIS, Nlets, NCIC and *Title 28*.

Training Objectives

At the conclusion of the TAC training class, the TAC will have an understanding of:

1. The responsibilities of the TAC as outlined by NCIC/CJIS/KCJIS
2. The training requirements of the full and limited access operators
3. Personnel screening requirements
4. NCIC System Quality Assurance
5. The proper use of III
6. Access to the NCIC Operating and Code Manuals
7. The on-line TAC Administration system (KACIS and OpenFox Configurator)
8. The resources available via the CJIS Launch Pad

OPERATOR TRAINING

All individuals that access NCIC terminals must be trained to ensure the efficient and effective use of the NCIC system. Basic training in the operation of the system shall be followed by certification and continued refresher classes throughout the operator's career.

To better accommodate the ongoing training process, the current full and limited access NCIC training PowerPoint's, produced by the KHP CJIS Unit, are available on the CJIS Launch Pad: https://cjisaudit.khp.ks.gov/launchpad/ under "CJIS Training > NCIC > NCIC Presentations".

Agencies are required to maintain documentation of any KCJIS/NCIC related training provided within the agency. This documentation is to be available for audit purposes.

A TAC (or alternate TAC) is to enter new user data into the nexTEST application on the CJIS Launch Pad immediately following the creation of the new user account within KACIS. The TAC must still advise the appropriate KHP CJIS Unit Trainer/Auditor of any new terminal users.

A TAC (or alternate TAC) is responsible for monitoring the certification status/expiration dates of the agency's terminal users via the expiration reports available within the nexTEST software application also accessed via the CJIS Launch Pad. When an operator's certification expires, NCIC access shall be denied until recertification is completed.

A TAC serving a full access agency must be no less than an NCIC full access certified terminal operator. Any TAC serving a limited access agency may choose to hold either a full access certification or a limited access certification.

Full Access Operator Training

Full access NCIC operators make entries, and inquiries, into NCIC. Newly hired full access NCIC operators must, within six months of employment or assignment, have initial training and be functionally tested and have their proficiency affirmed by a Kansas Highway Patrol CJIS Trainer/Auditor in order to assure compliance with NCIC policy and regulations.

Full access NCIC operators must be functionally re-tested, by their agency, and their proficiency reaffirmed every two years by the Terminal Agency Coordinator utilizing the on-line nexTEST software application which provides immediate scoring and feedback to the test taker. The user's certification status/expiration date will also be automatically updated upon the completion of the test.

Limited Access Operator Training

Limited access NCIC operators are persons whose responsibilities include inquiry capability to one or more components of the NCIC system. This operator does not have authority to enter, modify, clear, or cancel NCIC entries. The responsibility for training, functional testing and affirmation of proficiency of these operators according to their level of use, within the first six months of employment, lies with the terminal agency.

Limited access NCIC operators must also be functionally tested utilizing the on-line nexTEST software and have their proficiency reaffirmed by the agency every two years, following the initial training and testing period.

In the event of extenuating circumstances preventing any user from completing the test on-line, a TAC is to contact the assigned KHP CJIS Unit Trainer/Auditor.

Officer Training

Within twelve (12) months of employment or assignment, all sworn law enforcement personnel must receive basic training in NCIC matters. This training shall adhere to the minimum curriculum recommended by NCIC in order to ensure effective use of the system and compliance with NCIC policies and regulations. The minimum curriculum is to be included in KLETC training for new officers and all other law enforcement-training programs utilized for complying with Kansas statutes. All sworn law enforcement personnel shall be provided with continuing training concerning the NCIC/KCJIS system. Use of methods such as shift change briefings and in-service training are recommended to keep officers up to date in the proper operation of the system. ***Sworn personnel, who also function as terminal and/or mobile data operators, must additionally have their proficiency affirmed by means of certification according to their level of use.***

Other Criminal Justice Practitioner Training

The agency shall provide training appropriate to the level of access permitted of the NCIC system for all criminal justice practitioners other than sworn personnel. This may include persons such as record clerks, court clerks and district or county attorney office personnel who are not terminal operators. Resources for complying with this regulation are available from your regional KHP Trainer/Auditor.

Criminal Justice Administrator Training

Within six (6) months of election, selection or assignment, criminal justice administrators and upper level supervisory personnel must obtain training concerning the capabilities of the NCIC system, regulations, policy, audit requirements, sanctions and related civil liability problems. This training is designed to familiarize administrators with the key issues that affect their agency.

Training Materials

Training materials may be obtained from the CJIS Launch Pad or by contacting a KHP Trainer/Auditor.

PERSONNEL SCREENING

NCIC/STATE OF KANSAS STANDARDS

Personnel Access Requirements

A criminal justice agency is required to screen for employment, all personnel authorized to have access to CJI (Title 28, Code of Federal Regulations, part 20, subpart b.). Per the CJIS Policy, it is the responsibility of the agency's LASO to ensure that personnel screening procedures are being followed, though it may well be the TAC who is tasked with conducting the actual screening process. It is recommended the agency make only conditional offers of employment pending the completion of all records checks.

The KCJIS Policy and Procedure Manual states any employee or other individuals who are allowed to perform duties on behalf of a criminal justice agency in such a manner that may expose them to CJI in the course of their duties, to include reserves, interns, volunteers, consultants, vendors, contractors who will have authorized KCJIS access, or will have unescorted access to KCJIS computer terminal areas, or will have unsupervised access into computer software, hardware, or computer networks are required to be a U.S. Citizen or a non-U.S. citizen legally able to perform the work in or for the United States, at least 18 years of age and screened for a record of criminal activity and criminal history using a name based record check before employment is offered or before job duties are assigned that might expose them to CJI.

A fingerprint based check shall be conducted within 30 days after initial employment or assignment for all personnel who have direct access to CJI, and those who have direct responsibility to configure and maintain computer systems and networks with direct access to

CJI. This will include any support personnel, contractors or custodial workers who are enlisted to perform work on behalf of a criminal justice agency and will have authorized KCJIS access, or will have unescorted access to any agency computer terminal area, or will have unsupervised access into computer software, hardware, or computer networks.

Individuals who do not have authorized KCJIS access but may be working in an unescorted or unsupervised manner and could be inadvertently exposed to CJI shall be screened for a record of criminal activity and criminal history using a name-based record check.

RECORDS CHECKS

The name-based record checks must include the use of:

- The Interstate Identification Index (III),
- Kansas and other applicable states' Computerized Criminal History (CCH), and
- Local and Federal warrants (Kansas Warrant File and NCIC Wanted Person) check. (Only the message key "QWA" will return all NCIC warrants regardless of extradition limits).

Additionally, it is recommended any screening also include a driver's license check.

For a name-based records check, purpose code "J" shall be used when accessing CHRI on an employment applicant and other individuals who are engaged in the administration of criminal justice on behalf of the agency.

Purpose code "C" shall be used when accessing CHRI on other individuals enlisted to perform services on behalf of the agency, but are not engaged in the administration of criminal justice.

Information from both the name-based records check and fingerprint based records check, including diversions and expunged records, shall be used to determine eligibility to access KCJIS information as follows:

- The individual must not be a fugitive from justice.

- If a felony conviction of any kind exists, the hiring authority shall initially deny system access. The hiring authority may ask for a review by the CSO in extenuating circumstances where the severity of the offense and the time that has passed would support a possible variance.

- Adult misdemeanor convictions must be referred to the agency head for review and final determination.

- Any person adjudicated as a juvenile offender for what would be a felony or a serious misdemeanor, if committed, as an adult shall be referred to the agency head for final review and determination.

- Misdemeanor and felony diversions as an adult or juvenile successfully completed may not necessarily disqualify an individual, but must be referred to the agency head for review and final determination.

- Any misdemeanor diversion that is pending or has not been successfully completed may not necessarily disqualify an individual but, shall be referred to the agency head for review and final determination.

- Any felony diversions that are pending or have not been successfully completed will disqualify an individual.

- Any pattern of felony or misdemeanor arrests that have not resulted in convictions shall be referred to the agency head for final review and determination.

- The agency head may defer any determinations to the CSO at anytime.

If at any time, the CSO or agency head determines an individual's access would not be in the public's best interest, access to KCJIS may be denied.

Applicant fingerprint cards (blue in color) and records check results shall be secured separately from the agency criminal history records.

When the agency submits a fingerprint card, the person fingerprinted must be advised that the purpose of the fingerprinting is to check the criminal history records at the KBI Central Repository and the FBI national database.

If the information on the record is used to disqualify an applicant, the official making the determination of suitability for employment shall provide the applicant the opportunity to complete, or challenge the accuracy of, the information contained in the FBI identification record. The deciding official should not deny employment based on the information in the record until the applicant has been afforded a reasonable time to correct or complete the information, or has declined to do so. An individual should be presumed not guilty of any charge/arrest for which there is no final disposition stated on the record or otherwise determined. If the applicant wishes to correct the record as it appears in the FBI's record, the applicant should be advised that the procedures to change, correct or update the record are set forth in Title 28, CFR, section 16.34.

Employees and other individuals who meet the initial screening requirements shall also be re-screened on an annual basis via a name-based check. Individuals shall also be re-screened at any time the agency suspects the individual may have committed a potentially disqualifying act. Any re-screening must include the same name-based checks required at the time of employment. Additionally, it is recommended any annual re-screening should also include a driver's license check.

STANDARD OPERATING PROCEDURES (S.O.P.)

Pre-employment Records Checks

Your agency's S.O.P. shall include a reference to the effective completion of pre-employment records checks utilizing name based queries via III, Kansas and other applicable states' Computerized Criminal History (CCH) queries, fingerprint based checks and state and national warrant checks for all personnel who will have authorized KCJIS access, or will have unescorted access to a KCJIS computer terminal area, or will have unsupervised access into computer software, hardware, or computer networks.

Self-Reporting of any New Criminal Violation

Agencies must adopt a policy requiring any individual with authority to access KCJIS information to report to the agency head any new indictment, arrest, charge, conviction, or diversion of a criminal violation by the end of the business day following the reportable event.

Facility Security Procedures

The computer site, terminal area and/or any area where CJI is accessed or stored shall have adequate physical security to protect against unauthorized access.

Each criminal justice agency shall adopt operational procedures designed to ensure the physical security of criminal justice information in its custody and to prevent the unauthorized disclosure of such information. While agencies are free to develop their own physical security procedures the types of procedures recommended for consideration shall include:

- The establishment of physical barriers, sign-in procedures, guards or the use of keys, badges or technological locking devices to restrict access into secured areas.

- Segregation of terminals, files and other physical locations where CJI is used and displayed is necessary to prevent visual surveillance or eavesdropping.

Dissemination Guidelines

A basic review of agency dissemination guidelines shall be stated in the agency S.O.P. specifically addressing those instances when dissemination of <u>any</u> Criminal Justice Information (CJI) is allowed or prohibited. To include but not limited to III, CHRI, driver's license and registration information.

III/CHRI Access by/Transmission to Mobile Data Computers

Mobile data computers are allowed to query and receive detailed III/CHRI information. A record of criminal history on file may be transmitted to a mobile data computer. Your agency S.O.P shall address the usage of MDC's in accessing III/CHRI, if such access is allowed by your agency head.

Individual Access and Review of One's Own Criminal History

All individuals have the right to review and challenge their criminal history record information. However, a local agency is prohibited from providing KCJIS CHRI to an individual or the general public. The local agency shall instruct the individual to contact the KBI for Kansas Criminal History Record Information and/or the FBI or other state holding the record for III information.
The bases for implementation, of Individual Access & Review, are contained in K.S.A. 22-4704 and K.S.A. 22-4709. These procedures shall be simply described in an easy to follow format in the agency S.O.P. so that compliance with the statutes imposes no burden on either the agency or the person exercising this right.

Links are available on the CJIS Launchpad under CJIS Documents/Individual Access and Review including methods for accommodating challenge of the record, an administrative appeal and documentation for method of identification of the subject of the record.

NCIC Quality Assurance

The S.O.P. shall include the agency's requirements and procedures for entry, supplemental, modification, cancellation, clear, locate and inquiry of records. Reliance on NCIC manuals may be included on a secondary basis.

The use of entry worksheets is an audit requirement which shall be incorporated into the agency policy and procedures. Completed entry worksheets must be kept in the supporting case files.

An NCIC compliance requirement of complete, accurate and timely entries (within 3 days) implies that an agency shall place specific emphasis on the required documentation, proofing of entries and validation procedures. The exception is when any missing person (juvenile or adult) report is taken by an agency; the entry must be entered as soon as practical, once the minimally required information is obtained to make an entry, not to exceed 2 hours per Audit Standards.
In addition, temporary, final, amended and other protection from abuse orders must be entered immediately according to Kansas Statute.

Reporting of Violations of KCJIS Policy and Procedure Manual and Security Incidents

A policy violation occurs when agency personnel fail to follow KCJIS policy. If a violation of policy is discovered, the individual discovering the violation shall (1) take corrective action immediately and (2) notify the LASO and/or TAC immediately.

After discovery of a policy violation the local agency administration shall initiate an investigation to determine why the violation occurred, administer appropriate discipline and job performance counseling to all individuals involved, notify the appropriate KHP Trainer/Auditor and submit a report to the CSO documenting the violation and disciplinary or corrective measures that have been taken. If it is discovered a policy violation occurred at a local agency and the above process was not followed the CSO will open an investigation into the matter.

A security incident occurs when the operation or integrity of the KCJIS system is threatened. Threats include but are not limited to compromised assets, hacking and malware infections; the local agency employee that discovers the security breech shall immediately notify the agency LASO, other agency supervisory personnel, the State ISO and the KBI Help Desk. Steps shall be taken to identify, contain, isolate and document the incident as soon as possible.

Transfer or Removal of Personnel for Violations of local or KCJIS Policies

A criminal justice agency must have the authority to make sure that proper discipline is applied if personnel who have been screened subsequently violate security rules. Title 28, Subpart B, Section 20.21 (f) (4) ii, states that a criminal justice agency will *have the right to initiate or cause to be initiated administrative action leading to the transfer or removal of personnel authorized to have direct access to such information where such personnel violate the provisions of these regulations or other security requirements established for the collection, storage or dissemination of criminal history record information.*

KCJIS Access for Terminated, Resigned or Suspended Employees

In accordance with the KCJIS Policy and Procedure Manual, each agency shall develop formal written procedures for ending KCJIS access for employees who have resigned, are terminated or are placed on disciplinary or extended leave. The policy shall have some type of procedure for notifying the KBI Helpdesk so that the assigned token can be disabled immediately.

Agency Policy Governing E-mailing of Criminal Justice Information (CJI)

Criminal Justice Information may be transmitted when both the sending and receiving e-mail boxes belong to a domain approved by the FBI (such as leo.gov).

Agencies are also allowed to e-mail CJI from one agency to another IF the sending agency can ensure they are utilizing a NIST (National Institute of Standards and Technology) approved encryption program employing a minimum of 128 bit encryption. The agency's policy will need to properly reflect if such encryption is in place at the agency and the agency's intentions in relation to sending encrypted e-mails.

(*See Electronic Dissemination for further direction on emailing CJI.)*

Mobile Data Computer Usage and Physical Security

Written policies and procedures shall be in place governing the use and physical security of MDC's. Access shall be controlled by user ID's and passwords.

Agency has a Written Program to Train All Persons Having Access to KCJIS:

Within six months of election, selection or assignment all personnel with authorized KCJIS access shall be trained on privacy and security issues regarding CJI.

Criminal justice agencies shall adopt CHRI training programs. *"Each employee working with or having access to criminal history record information shall be made familiar with the substance and intent of these regulations"* (Title 28). Inadequate training in privacy, security, completeness and accuracy of criminal history record information, by an administrator of those who shall access the information, may result in the finding by a court that breach of a specific duty has occurred and the persons involved are liable for damages under the general principles of tort law.

The S.O.P. shall contain an organized training program that will include relevant federal, state and agency rules and regulations regarding the collection and dissemination of criminal history records and systems quality assurance. All employees with access to CHRI records shall be required to read all relevant policy documents.

Agency has a policy in place governing usage and access to NICS, and the appeals process.

Any agency conducting QNP transactions will be audited for their NICS usage and access. The OCA and NICS Transaction Number (NTN) are utilized during the audit process by the CJIS Audit Unit and shall be maintained with the agency's case file.

Agencies conducting QNPs should address any challenges (appeals) requested by persons who believe they have been wrongfully denied the transfer of a firearm based on a deny decision rendered by the agency.

All appeals of a denial decision must be made, in writing, to the NICS Section, at FBI directly. Literature on the appeal process (to include mailing addresses, telephone numbers and handouts for disseminating to denied subjects) can be found at http: www.fbi.gov/nics-appeals.

FURTHER CONSIDERATIONS AS AN AGENCY TAC

Expungement

Your agency may rarely, if ever, receive an order for the sealing or expungement of a criminal history record. It is highly recommended your agency address expungement procedures in your S.O.P. Only the custodian(s) of records shall have access to information expunged from a criminal history record. Personnel not authorized shall not be able to determine there is an expunged record when reviewing a subject's record. Expunged arrests are to be removed, blocked or hidden on a person's manual or computerized record. When sealing a record according to an order of expungement, all information supporting the arrest must be retrieved, placed in a new envelope along with the order of expungement and sealed. Obliterate the original file number and assign a new number if necessary. Expunged information must be flagged or filed separately to safeguard against release of information to unauthorized persons.

It is recommended any questions regarding expungements be referred to your agency's local legal representative or to the KBI Records Section.

Lost or Stolen KCJIS Equipment

If any KCJIS-related equipment is lost or stolen such loss shall be reported immediately to the KBI Help Desk so access through the affected equipment can be revoked.

If any equipment with CJI residing in it is lost or stolen, an official police report shall be filed and the agency shall retain documentation for audit purposes.

Escorting Visitors

The agency S.O.P. shall contain written procedures for escorting persons not normally authorized to enter the secured area.

Visitors shall be escorted at all times and checked with a name-based records check using purpose code "C".

The agency head shall have the ultimate authority to determine who is allowed access to the facility.

KCJIS Printouts – Handling, Storage and Disposal of Records

All CJI shall be securely stored to prevent access by unauthorized personnel.

Authorized personnel shall dispose of CJI in a manner to prevent access or recovery. KCJIS printouts must be protected from accidental observation and inadvertent disclosure when in active use. These printouts must not be left in open view when unauthorized persons are present. KCJIS printouts in active use must be transported and maintained under cover. Paper copies shall be shredded or burned.

Terminal Security

Computers must be configured in a way that requires users to log on and authenticate by means of a unique User ID and password. Terminals shall also be placed in such a manner as to prevent unauthorized persons from viewing the screen.

Logging On/Off

Users of KCJIS must log-on and log-off of the system at the beginning and end of their shift. Operators leaving the terminal for any period of time shall either lock their workstation or log off the system to prevent unauthorized access.

Three unsuccessful attempts to log into KCJIS will result in the user being denied access. The user's token will require a resynchronization with the server. This may be accomplished by having the user log into the KCJIS website with their UserID and token number (without the PIN) currently displayed in the passcode field. This will take the user to a second page, which will direct the user to wait for the token number to change (the number MUST be allowed to change) and then enter the entire Passcode consisting of the PIN and the token number being displayed. An alternative is for the user to wait 15 minutes and the token will be automatically resynchronized.

Any authorized KCJIS user needing access to KCJIS when his/her token is not functioning or is unavailable may obtain a temporary number or set of numbers from the KBI Help Desk. This password will only be valid during the user's current shift. The user's token will be disabled at this point and the KBI Help Desk must be contacted to re-enable it before its use can be resumed.

Storage of Agency CHRI

Title 28 does not protect agency records when they are maintained chronologically.
Chronological records, those filed by date and/or time, such as police blotters and jail logs are open to the public. Therefore, case files should be filed alphanumerically.

The regulations regarding dissemination of juvenile records are considerably more stringent than its adult record counterpart. Juvenile records must be flagged so they are readily distinguishable from adult records to alert the records person to its juvenile status or filed in a separate location to safeguard against an improper dissemination.

DISSEMINATION

Kansas CHRI / KORA

Two Kansas statutes deal with dissemination of information by public agencies. Most of the information dealt with in this manual concerns the application of the Kansas Criminal History Record Information Act, (CHRI) KSA 22-4701, et seq. Agencies need to be aware that the Kansas Open Record Act (KORA), KSA 45-215 through 45-223, also applies to this type of information. Quoting KSA 45-216, *(a) It is declared to be the public policy of the state that public records shall be open for inspection by any person unless otherwise provided by this act and this act shall be liberally construed and applied to promote such policy".* Whenever information is not restricted by the Kansas Criminal History Record Information Act, the general rule is that it must be made available to members of the public unless covered by other exceptions under KORA. Additional exceptions to the required disclosure under KORA are found in KSA 45-221. Questions regarding the release of information should be referred to your local legal representative or to the Kansas Bureau of Investigation, Central Records Repository, at (785) 296-8200.

Information that does not indicate a conviction is subject to restraints on dissemination. This non-conviction data is closed to the public, but it is possible for the record subject to review both conviction and non-conviction information by utilizing the process of Individual Access and Review.

Pending Process

Pending process information may also be disseminated. This information is defined as that related to an offense for which an individual is still actively in the criminal justice system. An arrest without a disposition which is less than one year old, the period of time during which a subject is serving a diversion, or an arrest that is still being actively scheduled for prosecution are examples of pending process information.

Non-Conviction Dissemination

Non-conviction data is for the most part considered to be information that is closed to the public and accessible to criminal justice agencies. Some form of legal authority such as a state statute or executive order, local ordinance, court ruling or order may authorize access to non-conviction data. In determining what information qualifies as non-conviction data, examples may include acquittals, dismissals, completed diversions non-prosecutable offenses, or charges pending prosecution. Records of arrest not accompanied by disposition that are more than one year old and in which no prosecution is actively pending may be included.

Who Can Receive KCJIS Information

Before CJI is disseminated, the person disseminating the information shall ensure the recipient is authorized to receive it. A sanction may be imposed on an agency or an agency employee for inappropriate or unauthorized dissemination.

Dissemination of NCIC Unrestricted Files Information

Dissemination of NCIC unrestricted files information is permitted to anyone upon request to confirm the status of a person and/or property (wanted or stolen only) provided such dissemination does not fall under the definition of commercial dissemination.

Agencies making inquiries on those seeking assistance from organizations such as homeless shelters, battered women shelters, churches or other charitable organizations must remain aware of the dissemination restrictions.

Any inquiry resulting in a hit on Supervised Release, National Sex Offender Registry File, Gang, Known or Appropriately Suspected Terrorist, Historical Protection Order, Violent Person, Identity Theft, Person with Information (contained in a NCIC Missing Person File entry), Protective Interest, NICS Denied Transactions and III are confidential and should be treated accordingly. The remaining NCIC Files are considered non-restricted files.

An OPT (Opt In or Opt Out) Field is a mandatory field in the NCIC Article and Vehicle Files to be utilized to indicate whether a record should be made available for dissemination via a publicly accessible website such as www.tracechecker.com .

"IN" will indicate that the record is available via the website while "OUT" will indicate the record is not available via the website. If an agency enters a specific date in the OPT Field, the record will not be made available for public dissemination until that date.

How KCJIS Information may be disseminated by Local Criminal Justice Agencies

Electronic dissemination:

CJI shall not be disseminated electronically, in any unencrypted format, except for the following:

a. Information from the National Weather Service or KHP road reports
b. Kansas humanitarian "attempt to locates", except when indicated it is intended for law enforcement release only.
c. NCIC unrestricted files information solely regarding wanted or stolen status.
d. Driver's license or other photos provided no personal identifying information (PII) accompanies the photo. Examples of PII include but are not limited to: Driver's license number, FBI number, KBI number, Name or Social Security Number.

CJI may be disseminated through an approved mobile data computer network that meets minimum encryption requirements, as outlined in the KCJIS Policy and Procedure Manual, to a mobile data access device having a KCJIS assigned mnemonic.

CJI may be disseminated by e-mail when both the sending and receiving e-mail boxes belong to one of the approved domains, i.e.; leo.gov. Agencies are also now allowed to e-mail CJI from one agency to another IF the sending agency can ensure they are utilizing a NIST (National Institute of Standards and Technology) approved encryption program employing a minimum of 128 bit encryption. A KHP CJIS Unit Technical Security Auditor must be contacted prior to implementing any e-mailing practices. Text messaging is prohibited.

Transmission of CHRI and intelligence information in audio format

Any electronic device that uses wireless or radio technology to transmit voice data may be used for the transmission of CHRI when an officer determines there is an immediate need for this information to further an investigation or there is a situation affecting the safety of an officer or the general public. Codes to disguise the voice transmission of non-conviction and arrest CHRI information shall be used.

Fax dissemination of Criminal Justice Information (CJI)

CJI may be transmitted by fax if both the sending and receiving agencies have valid criminal justice ORI's.

Internet or wireless fax transmissions are allowed under KCJIS Policy, but only when the encryption standards applied to e-mailing are met. A KHP CJIS Unit Technical Security Auditor must be contacted prior to implementing any such practice.

To prevent non-authorized personnel from viewing the data the sending agency shall call the receiving agency before transmission to ensure the person requesting the CJI will be present to receive the data to avoid any inadvertent dissemination.

Primary Dissemination

The requestor's name and the last three characters of the terminal operator's UserID are captured at the state level and retained on an automated log. Therefore the agency is not required to maintain a manual log of III or other CHRI inquiry transactions, however, an agency may choose to do so.

Secondary Dissemination

Any time Criminal History Record Information is shared with anyone outside of your agency a secondary dissemination log shall be kept. This log shall identify the secondary recipient, agency, date of dissemination, purpose of the dissemination, name and other identifiers of the subject of the record and the name of the person who generated the dissemination. These logs, whether automated or manual, shall be kept for a minimum of three years. There may be advantages to keeping the logs for a longer period of time.

Commercial Dissemination of State or Federal Records

The commercial dissemination of state or federal file records obtained from NCIC, driver's license, driver's license photographs and vehicle registrations obtained from the KCJIS/CJIS System is prohibited. Information derived for other than law enforcement purposes from national file records can be used by authorized *criminal justice* personnel *only* to confirm the status of a person and/or property (wanted or stolen only). Any advertising of services providing "data for dollars" is also prohibited. Any request for bulk data is prohibited. Authorized agencies are allowed to charge a processing fee for disseminating data for authorized purposes. The wholesale marketing of data for profit is not permitted, as in the example of a pre-employment screening or record check company requesting wanted person checks from NCIC to be conducted on individuals for various non-criminal justice employments.

Non-Criminal Justice Dissemination

Under the regulations, Title 28, 42 USC, K.S.A 22-4701, K.S.A. 38-1601, K.A.R. 10-12-1, non-criminal justice requestors are permitted to obtain conviction data but not non-conviction data. A criminal justice agency is not allowed to access III, or state level, criminal history records for a non-criminal justice requestor, i.e.; military recruiter, defense attorney or general public. Certain other requestors may be able to obtain sealed data or certain kinds of juvenile justice data. Agencies must not only have procedures in place to identify the agency and its purpose for the request but procedures which are designed to distinguish among different kinds of data and assure that only the proper data is disseminated.

Non criminal justice dissemination must also be logged. The logs must be maintained for a minimum of three years as well.

AUTHORIZED ACCESS BY A CRIMINAL COURT

In instances in which the prosecuting authority has not, for its own use, accessed III to obtain CHRI about the defendant or witnesses, a court cannot order the prosecutor or law enforcement agency to obtain and disseminate the III-derived CHRI to the defense counsel.

In these circumstances, if a judge wishes to access previously un-accessed CHRI of potential witnesses, he/she must issue an order to the FBI for the production of those documents.

The order to the FBI must be the original, must be signed by the judge, and must include the following information:

- Complete name and date of birth of the subject of the record
- Typed name of the judge
- Name and address of the specific court to which the response should be directed
- The ORI of the court

The mailing address for the order is:

Criminal History Analysis Team 1
BSS, CJIS Division
1000 Custer Hollow Road
Clarksburg, WV 26306

Upon receipt of the order, the FBI will conduct a search for any record pertaining to the subject(s) of the order and will forward any record(s) to the court at no cost. The judge may then release the information to the appropriate party, which may include the defendant and/or defense counsel as the court deems necessary.

ENTERING NEW USERS IN KCJIS AUTHORIZATION & CUSTOMER INFORMATION SYSTEM (KACIS)

Agency TAC procedures for entering new users shall be as follows:

- Go to KACIS, http://kacis.kcjis.state.ks.us/KacisSite/
- Log in with username and password
- Click on "User Admin" and select "Create New"
- Complete the text fields with the new user's identifying information
- Check the "Law Enforcement" box only if the new user is a sworn officer
- Click "Create" button at the bottom of the screen
- If identifying information submitted matches an existing record you will be presented with an option to select the already existing record or create a new person record (Only create a new person record if/when your new user is NOT actually the same person indicated in the existing record. Otherwise, select the existing record.)
- If the information submitted does not match an existing record, you will immediately be presented with the "Activate and Add Contact Information" section
- Note the auto generated KCJIS UserID for future reference (for assigning tokens, nexTEST & Configurator)
- Check the "Active" box if this user is ready for activation
- Most users will have "unassigned role" unless they are a TAC
- Enter Hire Date. This can be a future date of employment.
- Confirm the accuracy of name, DOB, DL number, LEO status and mother's maiden name
- Complete the e-mail, address and telephone number section if desired
- Click "Save" to save all data in these sections for this user
- Once a record is saved the data for the person you just created will be displayed
- Verify all data is accurate
- Click one of the "edit" links on the screen if modifications are needed
- Under "Authorized Applications" check the box next to "Central Message Switch" and "KCJIS Web Portal". (These boxes must be checked in order for the user to have access to OpenFox and the KBI's Web Portal.) The authorization for KsORT is approved through the KBI Help Desk directly, along with e-dispositions.
- Click Save

ASSIGNING AND ACTIVATING TOKENS

A UserID must be assigned in KACIS before this step can be performed.

- Go to the KCJIS website at: https://www.kcjis.state.ks.us
- Log in with your Username and Password
- Click on Help Desk
- Scroll down to SecurID Tokens and click on "Token Activity/Token Activity Form"
- Ensure your Agency ORI and shortcut are entered into the Agency and Shortcut fields
- Enter your first and last name in the TAC field
- Select an action from the drop-down box
    a. Broken – Use to report a token is broken or has failed. Describe the issue in the text field.
    b. Delete – This will move the token to "spare" status. This will not remove the UserID from KCJIS. The user will have to be set inactive separately in KACIS.
    c. Lost/Stolen – Describe the situation in the text field and follow up with an e-mail to the KBI Help Desk at helpdesk@kbi.state.ks.us stating circumstances and to whom it was assigned. If found the TAC must fax to the KBI a memo on agency letter head to have the token removed from lost status.
    d. New User – Use if a new KCJIS UserID is assigned a token for the first time:
        - On line A, enter the token serial number that you want assigned to this user, along with this user's name and UserID.
    e. Transfer – Use to transfer a token directly from one UserID to another:
        - Place the name and UserID of the prior user in line A and the identifiers of the intended new user in line B with the serial number of the token being transferred included on both lines.

      Transfer is also the action to be selected when a new token is being assigned to an active user to replace an expiring token:
        - Place the name and UserID of the user in both lines A and B with the serial number of the old (expiring) token noted on line A and the number of the new (replacement) token on line B.
- <u>For a new or returning user, the lower portion of the form must be completed</u>
- Though you may utilize the "Search Your Agency's Token Activity" function at the top of the Token Activity Form to retrieve/review previous token activity for your agency, you may wish to simply save a copy (electronic or paper) before submitting the forms.
- You will receive an acknowledgement advising the form was submitted successfully
- The user will then need to set up a PIN number for their token (see "Selecting a PIN")

The waiting period for the token activity form to be processed is up to 24 hours.

Should it be an emergency, you might be able to expedite the process by contacting the KBI Helpdesk at 785-296-8245.

SELECTING A PIN

The Token Activity form must be processed by the KBI before this step can be performed.

A PIN must be 4 to 8 digits. **CJIS policy will mandate that PINs be no less than 6 digits in the near future. Kansas will prepare for this change early and begin requesting 6 digits with new users immediately. Until the change takes full affect, KCJIS Web Portal dialog box requests will still reflect 4.**

- Operator opens Internet Explorer and goes to: https://www.kcjis.state.ks.us
- The RSA Secure ID screen will open
- Operator enters Username (KACIS assigned UserID)
- In the Passcode Box enter the number being displayed on the token
- Click Send
- The New PIN Page will be displayed
- Operator has the option of creating a PIN or accepting a system generated PIN
- It is recommended the operator click on the "I will create my PIN" button
- Enter the PIN selected, press TAB and enter the PIN again to confirm
- Try again if any of the following messages are displayed:
  "PIN and confirmation do not match" – "PIN must be ~~4-8 digits"~~ (6-8 digits) – "New PIN rejected"
- After successfully setting up the PIN, a web page appears to test the new PIN
- Type in the KCJIS User ID in the Username box
- In the Passcode box, type the PIN followed by the number being displayed on token
- Click Log In
- A SecurID Passcode page will appear requesting the KCJIS User ID and Passcode again
- Wait for the number on the token to change and then follow the instructions.

If you receive "Access Denied" you may have typed your Passcode incorrectly. Try again. If you again receive "Access Denied," call the KBI Helpdesk.

NAME CHANGES AND RE-HIRED EMPLOYEES

If a user changes his/her name (married, divorced) the user is not to be reentered into the KCJIS System with a new UserID. In these situations, the user's name should be modified in KACIS to reflect the change and a token activity form should be submitted so the user's name can be changed in the token database. For returning (re-hired) employees, simply reactivate the existing previous user account.

- Log into KACIS
- Hover pointer over the User Admin option located in the upper left corner of screen
- Click "Users" from the drop down menu
- Select the appropriate user by clicking on the UserID
- Confirm the appropriate user is selected and click on "Edit"
- Make changes that are necessary
  a. Activate/Deactivate User
  b. Change the KACIS Application Role (Unassigned Role or TAC)

c. Any changes to name, addresses, e-mail or telephone numbers
d. Application Authorization (Central Message Switch box or KCJIS Web Portal)

- Click “Save”
- Review the UserID information to confirm your changes have been saved

ASSIGN SECURITY ROLES IN OPENFOX CONFIGURATOR

A UserID must be assigned in KACIS before this step can be performed.

- Log into OpenFox
- Click on “Modules” in the upper right hand corner
- Select “Configurator”
- The “user” and “modify” buttons will already be selected. Simply click “OK”
- Type in the KCJIS UserID of the user
- Hit the enter key or click the “Get” button next to the UserID field
- Scroll to the bottom right corner to “Security Roles”
- Click on “search” button (binoculars)
- Double click on the security role you will assign
    - Full Access users require the “Full Access” option
    - Limited Access users require the ‘Query All” option
- Verify the appropriate security roles are assigned and click “Apply”
- You will receive a confirmation message (successful modify user request)
- Exit Configurator

Assign Security Roles to Multiple Users

Configurator has the ability of changing security roles for multiple users at one time. You must first prepare your Configurator setting to perform this task.

To adjust Configurator settings you must first log into OpenFox. This adjustment will only need to be made once. If you access Configurator on multiple KCJIS terminals, this setting will follow your login.

- Click on the Tools option from the desktop menu located at the top of the screen
- Click on the User Preference option from the dropdown menu
- Select “Configurator” from the choose a module section at the top of the screen
- Select the “Screen” tab
- Select the “Enable Global Record Screen” option under the Single/Global Record Screen
- Click the OK button in the lower right-hand corner of the screen

Assigning security roles via Global Configurator is done much like the single record Configurator

- The “user” and “modify” buttons will already be selected
- Click OK
- Click on the “search” button to populate all the users within your agency (the binoculars)
- Hold the “Ctrl” key down and click the users you wish to change

The user will be highlighted as you select them

- Click OK
- The list of users that will be affected by any changes you make will be in the left window
- Scroll to the bottom right corner to “Security Roles”
- Click on “search” button (binoculars)
- Double click on the security role you will assign
  - Full Access users require the “Full Access” option
  - Limited Access users require the ‘Query All” option
- Verify the appropriate security roles are assigned and click “Apply”
- You will receive a confirmation (successful modify user request)
- Click OK
- Click cancel and exit Configurator

REMOVING A USER

For persons no longer employed by the agency or no longer requiring access to KCJIS the TAC is required to:

- **In KACIS**
  Click “Deactivate” and then, to confirm, click the red “Deactivate” box that appears.

- **In OpenFox Configurator**
  Remove the security role(s)

- **In nexTEST**
  Change the user’s status to “Inactive”
  (Notify the appropriate KHP Trainer/Auditor of all personnel changes)

- **On the KCJIS website**
  Submit a “token deletion” form.

ORDERING TOKENS

Agency is to fax on letterhead stationary their request for tokens to Optiv Security Purchasing Department with the following information:

1. Quantity of tokens requested
2. Shipping address
3. Shipping contact name
4. Billing address (if different)
5. Purchase Order number (as applicable)

Fax:	303-298-0868
Office main line:	303-298-0600
E-mail:	tokens@optiv.com

The tokens are first shipped to the KBI for initial processing and then mailed to the agency. Please allow 2-3 weeks to receive tokens after order placement. If an agency does not receive their tokens within this time frame, the agency should contact the KBI Helpdesk at 785-296-8245 to confirm the status of the order.

Note: Expired, or otherwise non-functioning, tokens have no value and may be disposed of at the agency's discretion. Do not dispose of any token while it is still functioning.

KACIS AGENCY ADMINISTRATION

Modify Agency Information

It may become necessary to change information concerning your agency. These changes can include e-mail, addresses, phone numbers or building addresses for your agency.

To make changes to your agency:

- Log into KACIS
- Hover your pointer over the "Agency Admin" option located in the upper left corner of the screen
- Click "My Agency" from the drop down menu
- Click the "Edit Demographics" link in the upper left corner of the screen
- To add an e-mail, telephone or address click "Add New" and complete the information
- If changing current information change the information in the appropriate text box
- Click "Save"
- Review the information to confirm your changes have been saved

Viewing Lists of Users and Agencies

As a TAC you may view a list of users within your agency as well as a list of all agencies in Kansas.

- Log into KACIS
- Hover over "User Admin" to view a list of users within your agency or hover over "Agency Admin" to view a list of agencies in Kansas
- Click on "Users" (User Admin) or "Agencies"(Agency Admin) to view the two lists
- You may also perform a search for a specific UserID or ORI by typing your search criteria in the search box

Agency Demographic Validation

A validation of your agency demographic information is done through KACIS on an annual basis.

- 30 Days before your agency validation is due, you will be presented with a reminder to validate the “Agency Demographic Information”
- Once you have reviewed and updated your agency information click on the “Validate” button in the lower left-hand side of the screen
- If changes are needed click the “Edit” link to make appropriate changes
- Once you have updated your agency information click “Save”

If your agency validation is overdue, you will receive a message stating “Agency demographic information validation is required” and you must validate your agency information before navigation to any other screen within KACIS is allowed.

OPENFOX ARCHIVE AND RETRIEVAL CLIENT

- Log into OpenFox
- Click on “Modules” in the upper right corner
- Select “Archive Retrieval Client”
- Choose your start and end date (defaults to current date)
- If you choose to use a specific time frame place the time by hour/minute/seconds consecutively. i.e.; 09:15 would be 091500.
  (Not recommended…Setting a time frame will limit the search to those set hours for each date selected)
- You have two types of search options:
  Quick Search – 3 options
    - Search by Master Reference Index
    - Search by Terminal ID & Sequence #
    - String Search

  Detail Index Search – Search by specific parameters (most preferred search method)
    - Match all of the following (this is an “AND” type search)
    - Match any of the following (this is an “OR” type search)
- After clicking search, your results will return above your General Search Criteria
- You may have to resize the “Search Queue” window and/or use the vertical scroll bar
- Once the search is 100% complete, click on the specific line of the current search to open the search results

CJIS LAUNCH PAD

The CJIS Launch Pad, https://cjisaudit.khp.ks.gov/launchpad/, is an “open” website which does not require a VPN Remote or an RSA token. It may be accessed from any internet connected device. There are six applications and a “News and Information” window on the Home page. “CJIS Documents”, “CJIS Training” and “CJIS Links”, are open applications.
The other applications: CJIS Audit, CJIS Manuals and nexTEST do require a User Name and Password. When selecting one of the secured applications…

- You will encounter a login screen
- Use your 8 character KCJIS UserID as your User Name
- Your password is your agency's ORI with any letters in upper case

1. CJIS Audit

Clicking on CJIS Audit opens a window with the options of "Agency Login" and "Full Admin Login" and the agency TAC will select "Agency Login" which will produce the TAC Login window. Log in with your KCJIS UserID and for the initial log in password use your agency ORI then click "Login".
New questionnaires will be listed under "New Audits".

- Click the "Preview" icon for a list of all the questions and answer choices for each
- When the audit preview window is open, you may right click for the print option
- Click the "Start" icon to begin answering the questions
- Click on the appropriate answers
  - Multiple choice questions allow for one answer
  - Some questions include additional "Sub-questions" that are displayed when a certain answer is given
- Next, choose an action box
  - Save and Continue – Saves your answer and moves to the next question
  - Close and Finish Later – Does not save that answer. It will "bookmark" where you left off so you will be returned to the same question when you re-visit the audit
  - Skip Question – Will move to the next question. However, to complete the audit, all questions will need to be answered
  - Your progress through the questionnaire is tracked near the top of every window
- When you have answered all the questions you will be asked to:
  - Save for later – will require you to access the audit again to finalize
  - Review Audit – Opportunity to change your answers
  - Complete Audit – Forward to the KHP CJIS Unit for review
- Once answers are submitted the KHP CJIS Unit will review them and generate a report
- To view the status of the review process you can access the CJIS Launch Pad at anytime
- Once the CJIS unit report is posted you are to click on the "Response Required" button under "Status" to open the report
- If your agency's audit includes a data quality review of NCIC and/or Kansas Warrant File entries, the audit process will include a "Case File Review" document in addition to the questionnaire. Both require agency review/response(s)
- Use the edit button(s) to open text boxes to present your replies
- When completed with your review/replies, click "Save for Final Review" to resubmit
- The KHP audit unit will review and issue a final compliance report
- Access the CJIS Audit for your status
- Click "Review Final Notes" to view KHP CJIS Unit's closing comments and close the audit

Local agency TACs may access the Audit History at any time to review completed audits.

Administrator (TAC) Access for e-Notifications
(Only the TAC designated as the primary may make these changes.)

- Select “CJIS Audit” from the Launch Pad home page
- Click on “Agency Login” and enter the User Name and Password, click “Submit”
    - Use your 8 character KCJIS UserID as your User Name
    - Your password is your agency’s ORI with any letters in upper case
- Click “My Info”
- Any email address(es) appearing in the “Email Address” fields will receive notification by email of any impending audit assignments
- Multiple addresses may be input, but will need to be separated by a semicolon
- These e-notifications will arrive to the designated email address(es) once a week on Monday mornings (if such re-certifications are necessary)

2. nexTEST

User Access

To access his/her appropriate test for initial Limited Access certification, or the required biennial recertification for either Limited or Full Access, the user will select “nexTEST” from the CJIS Launch Pad home page

- Click on “User Login” and enter the User Name and Password
    - Use your 8 character KCJIS UserID as your User Name
    - Your password is your agency’s ORI with any letters in upper case
- The user will be presented with only the version of the test appropriate to his/her pre-set “Certification Level”
- Confirm the correct test is presented and click “Begin Test”
- Confirm your name is properly presented and again confirm the test presented is appropriate
- Click “Continue”
- Answer the questions presented (20 for Limited access and 50 for Full access)
- The user may minimize the test to the task bar and return to it. If the nexTEST program is closed, the user will have five (5) days to log-in and complete the test.
- Once all questions are answered, click “Grade Exam”. If any questions were missed, not answered, he/she will be advised to return to these questions
- Click “OK” to confirm you wish to submit your answers for scoring. The user will be advised that nexTEST is verifying the connection to the server and will submit your test for grading. Click “OK”
- The user will be advised immediately if the test is passed or failed and any questions answered incorrectly will be displayed along with the correct answer
- If the test is passed the user may print a certificate at this time
- Click “Logoff” to exit the nexTEST application

Administrator (TAC) Access for e-Notifications
(Only the TAC designated as the primary may make these changes.)

- Select nexTEST from the Launch Pad home page
- Click on “Agency Login” and enter the User Name and Password, click “Submit”
  - Use your 8 character KCJIS UserID as your User Name
  - Your password is your agency’s ORI with any letters in upper case
- Click “My Info”
- Any email address(es) appearing in the “Email Address” and “CC Email Address” fields will receive notification by email of any users who have certifications status(es) set to expire within the next 60 days
- Multiple addresses may be input, but will need to be separated by a semicolon
- These e-notifications will arrive to the designated email address(es) once a week on Monday mornings (if such re-certifications are necessary)
- All certifications will be included (full access, limited access, security awareness, LASO & TAC)

Administrator (TAC) Access for Expiration Reports

- Select nexTEST from the Launch Pad home page
- Click on “Agency Login” and enter the User Name and Password, click “Submit”
  - Use your 8 character KCJIS UserID as your User Name
  - Your password is your agency’s ORI with any letters in upper case
- Click “Reports”
- Click “Expiration Report”
- Utilize the drop down box at the top center of the resulting page to select which users you would like to display
- The default setting is to produce the expiration report for the current month but, for most agencies it may be preferable to select “All Dates in the Data Base” which is actually all users associated with the agency
- With the preference selected, click “Submit”
- The resulting list is, by default, arranged alphabetically but, the “Sort By” drop down box can be utilized to select to sort by “Expiration Date” which will place the expired, or nearest to expiration, users at the top of the list
- For larger agencies, the list of users may continue on additional pages and the user may select a specific page number or click “Next Listing” to view the next page

Administrator (TAC) Access for User Management

- Click on “Agency Login” and enter the User Name and Password, click “Submit”
  - Use your 8 character KCJIS UserID as your User Name
  - Your password is your agency’s ORI with any letters in upper case
- Select “User Management”
- User listings may be searched via Last Name, Username or by the first letter of the last name

- With a specific user identified, select the “History” icon to display the Test History and Training History tabs.
    - The Test History tab will display the test score and the “pass” or “fail” grade for the selected user in addition to indicating which test was completed.
    - If TAC wishes to print a certificate for the user’s file. This can be done here.
    - The Training History tab will provide the dates of any KHP sponsored classes the user has attended.
- With a specific user identified, select the “View” icon to display the “User Details” for the selected user including the username, agency, certification levels and expiration dates
- With a specific user identified, select the “Edit” icon to access/change the user’s password or status field

Adding New Users into nexTEST

- Click on “Agency Login” and enter the User Name and Password, click “Submit”
    - Use your 8 character KCJIS UserID as your User Name
    - Your password is your agency’s ORI with any letters in upper case
- Select “User Management”
- At the top of the next page, select “Add User”
- Complete the Add User form with all upper case letters with:

    - The new user’s name
    - The only choice available for ORI will be your agency’s
    - The default under “Certification Level” is “Awaiting Training”
    - Enter the date the new user was fingerprinted
    - Enter the KACIS assigned User Name
    - Enter a password and repeat for confirmation
      (Agency ORIs were utilized initially as “generic” passwords for all users)
    - The “Minimum Retest Time” is defaulted to “1 second”
    - “Status” is defaulted to “Active”
    - Check the box next to “CJIS Security & Awareness” for all users

- Once you have confirmed all data is entered correctly, click “submit” at the bottom of the form.

- Notify an appropriate KHP Trainer/Auditor of the addition of a new user at the agency, with the name and KACIS assigned User ID, and advise the auditor of the intended NCIC certification level, Limited or Full Access, for this new user.

For Limited Access users, the Trainer/Auditor will immediately set this certification level. New Full Access users must first attend the one day NCIC class presented by the KHP CJIS Unit, and successfully complete their initial Full Access test, prior to the Full Access certification level being assigned. The Limited Access level can be assigned to these users pending attendance for Full Access training/certification, at the agency’s discretion/request.

3. CJIS Manuals

User Name and Password will be required to sign in.

- Use your 8 character KCJIS UserID as your User Name
- Your password is your agency's ORI with any letters in upper case

- NCIC Operating Manual
- NCIC Code Manual
- NCIC TOU's
- KCJIS Policies and Procedures Manual

4. CJIS Documents (subject to change)

- Data Quality Audit Standards
- TAC Manual
- Technical Security Information
- CJIS Forms
- III & CHRI Transaction Log
- Individual Access & Review
- Kansas Warrant File
- KCJIS Trainer/Auditor Map with Contact Information
- KCJIS Broadcast Groups
- KCJIS Policy and Procedures
- NCIC
- News Bulletins
- NGI – Next Generation Identification
- Nlets
- REJIS
- Request for KCJIS Policy Review
- Secondary Dissemination Log
- Supplemental Entry, Maximum Number of Additional Identifiers Permitted
- Title 28 – Part 20

5. CJIS Training (subject to change)

- BLECO – Overview and Registration
- KCJIS Conference
- NCIC – Tests, PowerPoint presentations and worksheets
- TAC – PowerPoint presentations
- LASO
- Security Awareness Training
- KCJIS Training Schedule- TAC & NCIC
- Immigration Alien Query (IAQ)
- KCJIS Trainer/Auditor Map with Contact Information
- CJIS Launch Pad Overview
- Security Awareness for Non-Computer Users

6. CJIS Links (subject to change)

- KCJIS Secure Portal (token required)
- FBI CJIS Security Policy Resource Center
- National Weather Service Public Information
- Internet Crime Complaint Center (IC3)
- Law Enforcement Enterprise Portal (LEEP…for access to Law Enforcement On-Line [LEO])
- US-CERT (Computer Emergency Readiness Team)

NCIC VALIDATION PROCEDURES

NCIC policy requires that most NCIC records be validated between 60 and 90 days after entry and annually thereafter. The validation of NCIC records is now accomplished entirely on-line via OpenFox. The OpenFox Online Validation application streamlines the process by eliminating written reporting and mailing of documents. The application also dramatically reduces the chances of a valid file being accidentally purged (non-validated records are purged every 30 days) which could affect public and officer safety. Though the primary TAC is ultimately responsible for the completion of the validations, the process can be completed by any user at the agency as designated by the TAC.

The first Saturday of each month, when applicable, the agency will receive via the agency's primary OpenFox terminal, an automated notification of NCIC records due to be validated. These notifications will include records entered between 60 and 90 days prior and records entered in the same month for each prior year. (See the NCIC Manual Sec 3.4, 3 for the validation schedule).

There may be a series of notifications consisting of:

First notification – requires the record(s) be validated within 30 days

Second notification – notifying the agency that 20 days remain to complete and document the validation of the record(s)

Third notification – notifying the agency that 10 days remain

$.F – A "Failure to Validate" message listing any record(s) which have not been validated within 30 days of receipt of the first notification. This notice will be received on the Monday following the first Sunday of the month warning the agency to validate the record(s) or the NCIC system will retire the record(s) during the next purge cycle.

$.P – A "Purge due to Failure to Validate" listing any record(s) which have been retired from the NCIC system due to the agency's failure to document the completion of the validation process. This message is received the first Sunday of the month following receipt of a $.F message confirming that any record(s) not validated as required have been retired from the NCIC system.

If you are a Serving Agency for a non-terminal agency and/or a terminal agency which is not staffed/operational on a 24/7 basis, with an existing ORI User Agreement in which your agency has agreed to monitor KCJIS and receive unsolicited messages addressed to the KCJIS shortcut address and/or the ORI of the User Agency, it is the responsibility of the Serving Agency to forward or deliver any routine messages and/or notifications concerning validations to the Served Agency. For the non-terminal agencies, procedural agreements should be in place to effectively share the validation responsibilities between the Served and Serving agencies.

Validation requires the entering agency to confirm the record is complete, accurate and still outstanding or active. Validation is accomplished by reviewing the original entry and current supporting documents, including the officer's report. Recent consultation with any appropriate complainant, victim, prosecutor, court, motor vehicle registry files or other appropriate source or individual is required to ensure the validity, accuracy and completeness. The validation process includes a review of whether additional information has become available that could be added to the entry being validated. This would include running a new III, DMV and Kansas or out of state CCH inquiry to check for additional identifiers that may have become available since the date of entry or last validation of the record. If new identifiers are located, the record must be modified and the Validators Name (VLN) Field must be populated before validation is completed.

In the event the agency is unable to make contact with the complainant or reporting party, the agency shall make a determination based on the best information and knowledge available, whether or not to retain the original entry in NCIC. The determination by the agency to retain an entry in NCIC when contact with the party responsible for reporting the subject or property is unsuccessful means the agency is assuming liability for the entry.

The case file and documentation supporting an NCIC entry must be retrieved for a validation to be performed correctly. The NCIC entry worksheet is not sufficient for validating an entry because it may be inaccurate, reflecting transposing errors or misread information that occurred when it was entered on the worksheet. Every field of information on the worksheet originated from some other source. It is that source that should be used to validate the record.

The printouts or field notes supporting information entered in fields of an NCIC entry must be stored in the case file and reviewed during validation. The information must be compared against the data in the entry to determine that it is accurate.

TERMINAL USERS AGREEMENTS

User Agreements are located on the CJIS Launch Pad at:
https://cjisaudit.khp.ks.gov/launchpad//forms.htm
When your agency is updating or renewing agreements, please obtain the most current version of the form(s) from the above website. Some of the most commonly used KCJIS forms are:

Agency Connectivity Agreement KCJIS115
Inter-Agency ORI Use and Holder of Records Agreement KCJIS114
Records Check Agreement KCJIS114RC
NCIC Holder of Record Agreement KCJIS185
Management Control Agreement for Consolidated Dispatch KCJIS135

AGENCY CONTACT FORM KCJIS188

The KCJIS188 must be completed and faxed to KHP within five (5) business days of a change in agency head, and within three (3) days of an agency TAC and/or Alternate TAC change.

The KHP KCJIS Unit fax number is 785-296-0958. Once the KHP receives it, they will immediately fax a copy to the KBI, where the Help Desk staff will make the appropriate changes in the message switch programming. The KBI will complete the programming no later than 24 hours following receipt of the form at the Help Desk.

The signed KCJIS188 will also be used to update your agency's "Memorandum of Understanding for Kansas Criminal Justice Agencies Accessing the KCJIS Portal", as the KBI will attach it to your existing MOU on file at their office.

PUBLIC SAFETY INFORMATION SHARING NETWORK (Nlets)

What was previously known as the National Law Enforcement Telecommunications System (Nlets) is made up of representatives of law enforcement agencies from each of the 50 states, the District of Columbia, Puerto Rico, many federal law enforcement agencies and the National Insurance Crime Bureau (NICB). There is also a connection to the Canadian Police Information Center (CPIC) files. Nlets is a non-profit organization whose purpose is to provide interstate communications to law enforcement, criminal justice and other agencies involved in the enforcement of laws.

Nlets is comprised of eight regions with each region consisting of six or seven states and several federal agencies that are grouped together to represent a regional community of interest.

Nlets is a computerized, high-speed message switching system created for and dedicated to the criminal justice community. Its sole purpose is to provide for the interstate and/or interagency exchange of criminal justice and criminal justice related information. A log of all transactions is kept to provide system statistical reports and management information. Nlets is supported by a computer system located in Phoenix, Arizona. Administrative message traffic on the system includes all types of free form criminal justice related data from one point to one or more points. In addition, Nlets supports inquiry into state motor vehicle, driver’s license, criminal history and other state databases.

Each Nlets member must designate an agency as the control terminal agency (CTA). In Kansas, the Nlets CTA is the Kansas Bureau of Investigation. Any questions or problems relating to the Nlets system should be referred to the KBI at 785-296-8245.